REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims **1-35** are pending in the application.

Claims **1-35** have been rejected.

Claims **1-5**, **9-21, 26**, **28**, **31, 32,** and **34** have been amended in this submission. Applicants respectfully assert that the amendments to the claims add no new matter.

Claim **36-37** have been newly added in order to further define what the Applicants consider to be the invention. Applicants respectfully assert that no new matter has been added.

35 U.S.C. § 101 Rejections

In the Office action, the Examiner rejected claims 1 and all claims dependent thereon (claims 2-20 and 35) under 35 U.S.C. § 101 as not falling within a statutory category of invention. Applicants have amended claim 1 to clarify that the method covers a "for protecting the transfer of data between a computer and an external device." Accordingly, the claims as amended recite a method tied to a statutory category, e.g., a computer and/or an external device. In additional the method results in a transformation insofar as based on the determination of the claims, the data is transferred or blocked or otherwise modified. For example, claim 1 recites "determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication

session, wherein if said data communication session is to be allowed, then transferring the one or more data portions with data stored in the associated buffer, if any exist, toward or from the physical communication port, and if said data communication session is not to be allowed, then modifying data transportation related to said data communication session." Clearly, the communication of data between two devices (or blocking or modifying the communication) is a patentable method.

In the Office action, the Examiner rejected claims 21 and all intervening claims (22-34) under 35 U.S.C. § 101 as being directed to non-statutory subject matter and as directed to software per se. It is clear that software components comprise a large part of certain embodiments of the invention. Applicants have amended claim 21 to recite that the client agent is installed on a computer, thereby tying the client agent to patentable subject matter, i.e., a computer. Applicants further refer the Examiner to paragraph 12 in the application which reads:

It is respectfully submitted that the amendment does not narrow the scope of the claims. Applicants respectfully request that the rejection of claims 1-35 under 35 U.S.C. § 101 be withdrawn.

35 U.S.C. § 103 Rejections

In the Office action, the Examiner rejected claims 1-15 and 17-35 under 35 U.S.C. § 103(a), as being unpatentable over Nickles (US Patent No. 6,134,591) in view of Hann et al (US Patent No. 4,799,153). Applicants traverse the rejection for at least the reasons that follow.

The Nickles reference discloses "a network security system that has a single point of access control to a source computer system." (Abstract, emphasis added). In particular, the Nickles reference discloses:

> An indication is received that a first user of a first computer program module desires to communicate with a destination computer system. When this indication is received, a message is directed to a security computer system. The security computer system determines whether the first user is authorized to access the destination computer program

> module of the destination computer system. If the security computer system determines that the first user is authorized to access the destination computer system, the security computer system sets up a communication protocol between the first computer program module and the second computer program module. (Abstract, emphasis added).

Preliminarily, one distinction between the Nickles reference and the claims of the present application is that the Nickles reference is directed to securing an access of a user to a computer in a network (or a program module thereon), whereas the pending claims are directed to securing a transfer of data between a computer and an external device connected to the computer.

In rejecting claim 1, the Examiner pointed to the abstract; however, as clearly demonstrated by the above, the Nickles reference is not in fact directed to securing transfer of data related to a computer and an external device connected to the computer.

To find the element of "receiving a data portion during a data communication session..." the Examiner pointed to the Nickles reference, column 11 lines 60-63, which recites:

> When the gateway component of the web server 32 receives the message 4, the gateway component prepares the program modules to receive data from the object using information provided in message 4. (Nickles, col. 11, lines 60-63).

However, message 4 described by the Nickles reference is not the data portion during a data communication session. Rather, the message as taught by the Nickles reference comprises various information related to the session, e.g., port number, time related values, etc.

In fact, the message analyzed in the Nickles reference is sent and received prior to establishing the actual session involving communication of data to be transferred. Rather, the message analysis is used merely as part of a process of determining whether the session is to be allowed to commence. Then, once a user has been authenticated, data is transferred freely, and data portions related to the communication session are neither captured nor analyzed.

Accordingly, the Nickels reference does not teach or disclose "receiving . . . a data portion during a data communication session between the computer and the external device," as recited in claim 1.

Next, to find the element of ". . .the data portion being associated with a particular physical communication port of the computer and with the device that is currently communicating via the particular physical communication port," the Examiner points to column 9 line 1-2 of the Nickles reference, which recites:

> The security server 24 communicates with external computer systems or devices via the I\O port 85. The security server 24 provides a single point of control for performing the security and administration services of the network security system 10. (Nickles, col. 9, lines 1-5, emphasis added).

As such, server 24 receives various messages from other computers operated by users attempting to access the network. Accordingly and as taught by Nickles, the messages received by server 24 relate to authenticating users. However, the Nickles reference does not teach or disclose "receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device, said external device connected to the computer and communicating therewith via a physical communication port," as recited in claim 1.

The Examiner further points to column 3 lines 36-42 of the Nickles reference, which recite:

> Also, setting up the communication protocol may include selecting, in response to the step of receiving the electronic communication, one port of the multiple ports of the source computer system to be used for communication of information over the computer network between the first computer program module and source computer system. The first computer program module communicates with the source computer system via the selected one port and the source computer system communicates with the first computer program module via the one port. The one port is preferably selected by a randomizing selection program module. (Nickles, col. 3, lines 36-42, emphasis added)

Nickles teaches generating random port assignments for communication between devices (see Abstract). Accordingly, the Nickles reference teaches selecting software

ports for a communication session. However, such port selection is unrelated to a physical communication port (e.g., a USB port). Accordingly, the Nickles reference does not disclose "analyzing, by said module, the data portion according to a protocol associated with the physical communication port," as recited in claim 1.

In addition, the Nickles reference does not disclose "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, wherein if no decision may be reached on whether to allow, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd'," as recited in claim 1.

The Examiner concedes that Nickles does not disclose "... if not storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for the next data portion, if yes, proceed to step 'd'" and "determining whether to allow the data communication session, if yes transferring the one or more data portions with data that are stored in the associated buffer, if any exist, toward or from the physical communication port, if not, modifying the data transportation," as previously recited in claim 1.

The Examiner points to the Hann reference for this element. The Hann reference discloses:

> Security of communications in a packet-switched data communications system is enhanced by introducing terminal and host security devices into the system in communicative relationship with a terminal and a host processor, respectively. In response to a user-initiated data entry at the terminal, the terminal security device generates an initial data packet indicative of user authorization or not, but which is unsuited for processing by the addressed processor, ahead of additional data packets containing user-entered message data to be processed by the addressed processor. The host security device intercepts and processes the initial data packet and, if user authorization is indicated therein, replaces it with an artificial data packet solely to render the additional packets amenable to processing by the addressed processor and thereby to

> establish a communications session between user terminal and processor-associated database to which access was requested. (Abstract, emphasis added).

Therefore, the Hann reference – like the Nickles reference – is directed to securing a communication between a terminal and a computer, and specifically, to authenticating users, not data being communicated or transferred.

Hann is directed to a packet-switched data communications system. Hann teaches operating at the data layer, e.g., drop or forward packets as known in the art but does not teach buffering in order to process information at higher layers or according to higher level protocols.

In particular, the Examiner pointed to column 11, lines 48-56 of the Hann reference:

> Each LAPB controller generates an interrupt upon receiving a level 2 acknowledgment of a transmitted frame, receipt of an error-free frame, or upon the occurrence of an error condition. Each LAPB controller, contains an interface to DMA transfer Bus 322. Each LAPB controller transfers data to or from the buffer storage 320 via data bus 326 using the direct memory access capability of the WD2511 integrated circuit. (Hann, col. 11 lines 48-56).

Accordingly, the Hann reference teaches utilizing an initial data packet indicative of user authorization, and enabling (or not enabling) a communication session by replacing data in such initial packet.

As taught by Hann, a buffer is used by a Link Access Procedure, Balanced (LAPB) controller as known and common in the art. However, the Hann reference does not disclose (either at col. 11, lines 48-56 or elsewhere) conditionally storing data in the buffer. Rather, a buffer as taught by Hann is part of a standard interface with a DMA or other components.

Accordingly, the Hann reference does not teach or disclose "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, wherein if no decision may be reached on whether to allow, then storing the data portion in a buffer, wherein the buffer is associated

with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd'," as recited in claim 1.

Accordingly, claim 1, and all claims dependent therefrom, are allowable over the Nickles and Hann references.

In addition, although claims 2-21 and 35 are allowable as depending from an allowable base claim, Applicants wish to add further comments regarding certain features of these claims.

Regarding claim 2, neither Nickles nor Hann teach "wherein the step of modifying the data transportation comprises blocking the transportation." As discussed, since the cited references do not modify (or otherwise handle) the actual data, they consequently do not block a session based on the data communicated over the session.

Regarding claim 4, Applicants respectfully assert that translating a CGI format to another format (as disclosed by Nickeles) does not disclose "wherein the step of modifying the data transportation comprises modifying a status of a requested file," as recited.

Regarding claims 6-8, 11, 15 and 18, although I\O ports are mentioned by Nickles, such ports are mentioned as part of a general design of a computer. However, as discussed above, the Nickles reference does not disclose manipulating and/or handling data associated with such specific ports.

Regarding claims 9-10, the Nickles reference does not disclose analyzing the data portion as recited. As discussed, neither the Nickles nor the Hann reference analyzes data portions of a communication session.

Regarding claims 12-14, processing of the initial packet as taught by the Hann reference is unrelated to any other packet or data stored in a buffer.

In addition, Applicants have added claims 36 and 37 that recite elements of "wherein determining whether a decision on whether to allow the data communication session may be reached is based on a plurality of data portions wherein at least one of said plurality of data portions is stored in said buffer" and "wherein determining whether to allow the data communication session is based on a plurality of data portions wherein at least one of said plurality of data portions is stored in said buffer." The Hann reference does not disclose these elements.

Accordingly, claim 1, and claims 2-21 and 35-37, which depend therefrom, are allowable over the the Nickles and Hann references.

Similar distinctions are applicable to independent claim 21 and claims 22-34 which depend therefrom. Accordingly, claim 21, and claims 22-34 which depend therefrom, are allowable over the Nickles and Hann references.

In the Office action, the Examiner rejected claim 16 under 35 U.S.C. § 103(a), as being unpatentable over Nickles in view of Hann et al. and in further view of Cheng et al. (US Patent No. 6,769,071). Applicants traverse the rejection for at least the reasons that follow.

In light of the discussion above, claim 16 is allowable at least for being dependent from an allowable base claim. Furthermore, the Cheng reference can not cure the deficiencies of the Nickles and Hann references as discussed above. Accordingly, for this additional reason, claim 16 is allowable over the combination of the Nickles, Hann and Cheng references.

In view of the foregoing amendments and remarks, Applicants assert that the pending claims are allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

Please charge any fees associated with this paper to deposit account No. 50-3355.

Respectfully submitted,

/Guy Yonay/
Guy Yonay
Attorney/Agent for Applicants
Registration No. 52,388

Dated: April 15, 2010

Pearl Cohen Zedek Latzer, LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801